

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-105612

(43)Date of publication of application : 24.04.1998

(51)Int.Cl. G06F 17/60

(21)Application number : 08-260757

(71)Applicant : FUJITSU LTD

(22)Date of filing : 01.10.1996

(72)Inventor : NAKAMURA KIMIHARU
EYA TAMEYUKI
KANDA YASUNORI

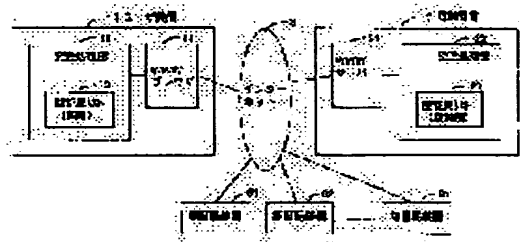
(54) AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To allow a user to easily select an authentication station out of plural authentication stations by executing the electronic settlement of accounts while using a key issued by a common authentication station included in the list of authentication stations contracted by the owner of a server and the list of authentication stations contracted by the user of client equipment.

SOLUTION: Respective authentication station devices 61-6n issue respectively independent public keys to contracted users and shops. Therefore, when a certain user or shop respectively contracts two authentication station devices 61 and 6n, that user or shop is to have two public keys respectively.

Accordingly, when the user executes ordering processing through a network to a certain shop, without confirming whether the user himself contracts the same certification station device or not, the electronic settlement of accounts is enabled by using the public key issued by the mutually common certification station device while utilizing two certification station lists 13 and 23. Thus, the user can easily select the authentication station device.



THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-105612

(43)公開日 平成10年(1998) 4月24日

(51)Int.Cl.⁶

G 0 6 F 17/60

識別記号

F I

G 0 6 F 15/21

3 4 0 B

3 3 0

審査請求 未請求 請求項の数 4 O L (全 9 頁)

(21)出願番号 特願平8-260757

(22)出願日 平成8年(1996)10月1日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(72)発明者 中村 公治

大阪府大阪市中央区城見二丁目1番61号

富士通関西通信システム株式会社内

(72)発明者 江谷 為之

大阪府大阪市中央区城見二丁目1番61号

富士通関西通信システム株式会社内

(72)発明者 神田 恭典

大阪府大阪市中央区城見二丁目1番61号

富士通関西通信システム株式会社内

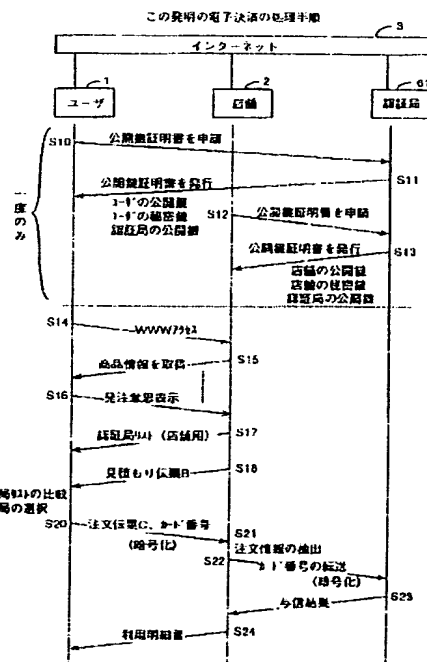
(74)代理人 弁理士 野河 信太郎

(54)【発明の名称】 認証システム

(57)【要約】

【課題】 この発明は、認証システムに関し、ユーザが利用可能な認証局が複数個ある場合でも、容易に利用する認証局を選択できる認証システムを提供することを課題とする。

【解決手段】 ネットワークを介して接続されたクライアント装置とサービス提供サーバとからなる電子決裁の認証システムにおいて、クライアント装置が、サービス提供サーバから送信されるサーバの所有者が契約している認証局のリストと、クライアント装置のユーザが契約している認証局のリストとを比較し、両リストに含まれる共通の認証局を選択して、この認証局が発行する鍵を用いて電子決裁を行うことを特徴とする。



ユーザと店舗で同じブランドを
見つけ、そのブランドを選択して
決裁を行う

【特許請求の範囲】

【請求項1】 ネットワークを介して接続されたクライアント装置とサービス提供サーバとからなる電子決裁の認証システムにおいて、

クライアント装置が、サービス提供サーバから送信されるサーバの所有者が契約している認証局のリストと、クライアント装置のユーザが契約している認証局のリストとを比較し、両リストに含まれる共通の認証局を選択して、この認証局が発行する鍵を用いて電子決裁を行う認証システム。

【請求項2】 前記サービス提供サーバが、サーバの所有者が契約している認証局のリストを作成する第1の作成手段と、この作成された認証局のリストを前記クライアント装置へ送信する第1の送信手段とを備え、

前記クライアント装置が、前記第1の送信手段によって送信された認証局のリストを受信する第1の受信手段と、

クライアント装置のユーザが契約している認証局のリストを作成する第2の作成手段と、

ユーザの契約している認証局が発行した鍵を記憶する鍵記憶手段と、

前記第1の受信手段によって受信された認証局のリストと前記第2の作成手段によって作成された認証局のリストとを比較して共通する認証局を選択する比較手段と、前記比較手段によって選択された認証局が発行した鍵であって、かつ前記鍵記憶手段に記憶されている鍵を用いて電子決裁情報を暗号化する暗号化手段と、

暗号化された電子決裁情報をサービス提供サーバへ送信する第2の送信手段とを備えることを特徴とする請求項1記載の認証システム。

【請求項3】 前記サービス提供サーバが、前記クライアント装置から送信された電子決裁情報を受信する第2の受信手段と、

受信した電子決裁情報を復号化する復号化手段と、

復号化された電子決裁情報を用いて受注処理を行う受注手段とをさらに備えることを特徴とする請求項2記載の認証システム。

【請求項4】 前記クライアント装置が、前記第2の作成手段によって作成された認証局のリストに含まれる複数の認証局に選択優先度を付与する優先度付与手段をさらに備え、

前記比較手段が選択した共通の認証局が複数個存在する場合に、選択優先度の最も高い共通の認証局のみを抽出することを特徴とする請求項2記載の認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、認証システムに関し、特にネットワークを利用した取引や売買、サービスの授受を実現する場合に必要となる、電子決裁上の認証を行う認証システムに関するものである。最近、イン

10 【0002】

ターネットの World Wide Web (以降WWWと称する)を利用して、ネットワーク上の取引(電子ショッピングや電子商取引)が実現されつつある。このようなネットワーク上の取引では、商品又はサービスを提供する店舗・業者と消費者などのユーザは取引や売買を直接対面して行うことができない。したがって、ユーザの身元の保証と、サービスを提供する業者(電子ショッピングなら店舗)の身元保証をいかに行うかが、安全に取引や売買を行う上で大変重要である。

【従来の技術】 クライアントーサーバ型の形態をとるネットワークを利用した電子商取引において、サーバ側からクライアント(ユーザ)の認証を行う場合、現状では公開鍵暗号方式をベースとした認証を行うのが一般化しつつある。すでに実用化されているクレジットカード決済では、SET(Secure Electronic Transactions)やSTT、SEPPなどの電子決裁技術が有名である。

【0003】 電子決裁の一例として、SETを用いた場合のクレジット決裁の従来例を以下に示す。図6は、ユーザ及び店舗の認証を行い、インターネットを利用してユーザがその店舗から商品を購入するクレジット決裁の手順を示したものである。ここで、ユーザ101、店舗102及び認証局103は、インターネット100を経由して接続されているものとする。ユーザ101、店舗102及び認証局103には、それぞれパソコン等の端末にこのようなクレジット決裁するのに必要なソフトウェアが組み込まれる。認証局103とは、クレジット決裁を利用するユーザ又は店舗等の利用者の身分を公正・中立な立場で電子的に証明する第三者の機関であり、たとえばクレジット会社がこの認証局(Certificate Authority)を運営している。

【0004】 認証局103は、一般的に次のような業務を行うものである。

- 1) 利用者の身分を確認して、その登録・管理をすること。
- 2) 利用者に「公開鍵証明書」を発行すること。
- 3) 公開鍵とこれと対となる秘密鍵の生成、更新、利用者に公開鍵及び秘密鍵の配送をすること。
- 4) 否認防止のための発信及び受信の証明と内容の証明をすること。
- 5) 通信目録の作成、鍵のコピーの管理及び再発行、これらの記録管理をすること。

【0005】 ここで「公開鍵証明書」とは、利用者(公開鍵の持主)の電子的な身分証明書である。この中には、利用者を特定するための名前などの登録情報、利用者に与えられる公開鍵が含まれ、認証局自身の秘密鍵によるデジタル署名が付与されている。このデジタル署名が付与されているため、「公開鍵証明書」は、利用者でない他者が公開鍵証明書を偽造することはできない構造となっている。

【0006】したがって、以下に述べるような従来のクレジット決済の手順を実行するためには、ユーザ101と店舗102とが同じ認証局からそれぞれの公開鍵の証明書を発行してもらっていることが必要である。

【0007】図6において、S100からS103の手順は、郵送等のオフライン手段を使用して行われる。すなわち、ユーザ101及び店舗102は、認証局103に自己の公開鍵を発行してもらうために、書類の郵送等により「公開鍵証明書」の申請を行う（S100、S102）。この申請を受理した認証局103は、書類審査などで身元の確認を行った後、ユーザ101及び店舗102に対して「公開鍵証明書」を郵送する（S101、S103）。

【0008】「公開鍵証明書」を受理したユーザ101及び店舗102は、クレジット決済を実行するために、「公開鍵証明書」に記載されている情報及び対となる秘密鍵をそれぞれクレジット決済を実行するパソコンに入力しておく。たとえば、ユーザから送信される情報を暗号化するために公開鍵証明書と秘密鍵が入力され、パソコンのハードディスク等に記憶される。

【0009】S104からS111が、従来行われているクレジット決済によって実際に商品購入を行う処理である。まず、ユーザ101が、インターネット100を経由して、店舗102のWWWブラウザにアクセスする（S104）。

【0010】そして店舗102は、アクセスのあったユーザ101に対してその店舗102の所有する商品情報などを送信する（S105）。その後、商品情報を取得したユーザ101は、自己の望む商品が決定したら、発注意思表示のデータを店舗102へ送る（S106）。そして店舗102は、この発注意思表示に対して見積もり伝票をユーザ101へ送信する（S107）。見積もり伝票を受理したユーザ101は、必要な数量などを記入した発注伝票とクレジットカード番号等を店舗102へ送信する（S108）。店舗102は、発注情報のみを抽出して、残りのクレジットカード番号など認証に必要な情報を認証局103へ転送する（S109）。認証局103では、この決済に必要な情報を確認後、認証が完了したか否かを示す受信結果を店舗102へ返信する（S110）。受信結果を受信した店舗102では、認証が正常に完了した場合には、利用明細書をユーザ101へ送信する（S111）。以上によってクレジット決済による商品購入が完了する。ただし、ユーザの契約している認証局と店舗の契約している認証局が異なる場合などは、認証が正常に行えないため、認証不可の受信結果が送信され、クレジット決済は成立しない。

【0011】

【発明が解決しようとする課題】従来、このようなネットワークを介した電子的なクレジット決済を利用せずに、ユーザが店舗に出向いて「クレジットカード」の現

物を店舗に提示してクレジット決済をする場合にも、ユーザ及び店舗の双方が同じクレジット会社と契約していることが前提となっている。同様に、前記したネットワークを介した電子的なクレジット決済でも、ユーザ及び店舗の双方が同じクレジット会社と契約していることが前提となる。すなわち、前記したような電子的な決済や認証を用いたとしても、ユーザも店舗もある認証局と個別に契約を結ばなければならない。

【0012】認証局が一つしか存在しない場合には、必ずユーザと店舗が同じ認証局による認証を受けるので問題とはならないが、複数の認証局が存在する場合には、ユーザと店舗が契約を結ぶ認証局が異なる場合があるので、クレジット決済が不可能な場合があり得る。現実には、クレジット会社は複数社存在するので、クレジット会社が運営する認証局も複数存在しうる。したがって、ユーザも、店舗も複数のしかも任意の認証局と契約しているという状態が想定される。このような状態において、ユーザがクレジット決済を行おうとする場合は、次のような問題点が発生する。

【0013】1) ユーザが購入したい商品を販売している店舗が契約している認証局が、そのユーザが契約している認証局の中に含まれているか否かを、ユーザが常に確認する必要がある。

2) また、店舗が契約している認証局は一般に異なるため、購入する店舗を変更する場合には、その都度店舗が契約している認証局をユーザが確認する必要がある。

3) クレジット会社が認証局を運用すれば、クレジット会社の認証利用特典などのために、ユーザは電子取引にて利用可能な認証局のうち、自分の好みの認証局を選択する煩わしさが発生する。

【0014】この発明は以上のような事情を考慮してなされたものであり、上記3つの問題点を解決することを課題とし、ユーザが複数の認証局と契約している場合にも、ユーザが容易に認証局を選択することのできる認証システムを提供するものである。

【0015】

【課題を解決するための手段】この発明は、ネットワークを介して接続されたクライアント装置とサービス提供サーバとからなる電子決済の認証システムにおいて、クライアント装置が、サービス提供サーバから送信されるサーバの所有者が契約している認証局のリストと、クライアント装置のユーザが契約している認証局のリストとを比較し、両リストに含まれる共通の認証局を選択して、この認証局が発行する鍵を用いて電子決済を行う認証システムを提供するものである。

【0016】また、サービス提供サーバが、サーバの所有者が契約している認証局のリストを作成する第1の作成手段と、この作成された認証局のリストを前記クライアント装置へ送信する第1の送信手段とを備え、前記クライアント装置が、前記第1の送信手段によって送信さ

れた認証局のリストを受信する第1の受信手段と、クライアント装置のユーザが契約している認証局のリストを作成する第2の作成手段と、ユーザの契約している認証局が発行した鍵を記憶する鍵記憶手段と、前記第1の受信手段によって受信された認証局のリストと前記第2の作成手段によって作成された認証局のリストとを比較して共通する認証局を選択する比較手段と、前記比較手段によって選択された認証局が発行した鍵であって、かつ前記鍵記憶手段に記憶されている鍵を用いて電子決裁情報を暗号化する暗号化手段と、暗号化された電子決裁情報をサービス提供サーバへ送信する第2の送信手段を提供するものである。

【0017】さらに、前記サービス提供サーバが、前記クライアント装置から送信された電子決裁情報を受信する第2の受信手段と、受信した電子決裁情報を復号化する復号化手段と、復号化された電子決裁情報を用いて受注処理を行う受注手段を備えてもよい。ここで、前記クライアント装置が、前記第2の作成手段によって作成された認証局のリストに含まれる複数の認証局に選択優先度を付与する優先度付与手段をさらに備え、前記比較手段が選択した共通の認証局が複数個存在する場合、選択優先度の最も高い共通の認証局のみを抽出するようにしてもよい。

【0018】ネットワークの対象としては、世界中の各種サーバ、パソコン等が多数接続されるという点で見れば、インターネットが最も好ましいが、これに限定されるものではなく、その他のWAN、LAN等であってもよい。クライアント装置は、ネットワーク接続機能を有したパソコンやワークステーションを用いることができる。サービス提供サーバは、主として店舗、営業所等に設置され、提供するサービスの規模に応じてワークステーションやパソコンを用いればよい。

【0019】この発明で対象となる認証局のリストは、「クライアント装置側のユーザ、すなわち購買者が契約した認証局」のリストと、「サービス提供サーバ側の所有者、すなわち業者・店舗が契約した認証局」のリストの2種類がある。

【0020】認証局とは、たとえばクレジット会社をさし、ユーザ及び店舗の身元を電子的手段を用いて認証する機能を有するものである。ここでも、この認証機能を実行する装置は、通常パソコンやワークステーションなどのコンピュータが利用され、認証に必要なデータは厳格な管理下におかれる。したがって認証局としては、クレジット会社自体の他、公的機関あるいは、信頼のおける第三者機関が運営する場合もある。

【0021】以上、述べたクライアント装置、サービス提供サーバの各手段の機能は、通常、パソコン等に内蔵されたソフトウェアと、CPUを中心とするハードウェアによって制御される。また、クライアント装置及びサービス提供サーバとも、マンマシンインタフェースとし

て、キーボード等の入力装置、CRT、プリンタなどの出力装置を備えることが好ましい。

【0022】電子決裁を行う場合に、クライアント装置とサービス提供サーバ間を転送される電子決裁情報は、通常安全のため暗号化される。この暗号化のために、一般的に認証局が発行する「鍵」と呼ばれるデータが用いられる。この鍵として、たとえば、1組の「公開鍵」と「秘密鍵」を用いる方法がある。

【0023】

10 【発明の実施の形態】以下、図面に示す実施の形態に基づいてこの発明を詳述する。なお、これによってこの発明が限定されるものではない。図1は、この発明の認証システムの基本構成ブロック図である。ユーザ装置1は、ユーザ側に設置される装置であり、たとえばパーソナルコンピュータ（パソコン）のような装置である。店舗装置2は、店舗側に設置される装置であり、商品やサービスを提供するサーバである。認証局装置61、62……6nは、たとえばクレジット会社が運営する装置であり、公開鍵の発行や管理を行う装置である。

20 【0024】ユーザ装置1、店舗装置2、認証局装置（61……6n）は、インターネット3に接続され、インターネットの汎用通信プロトコルを実行するためのハードウェアとソフトウェアを備える。また、ユーザ装置1及び店舗装置2は、通信される情報の表示、入力、出力等のために、WWWブラウザ11、21を備えることが好ましい。

30 【0025】ユーザ装置1は、店舗装置2から送られてくる情報をWWWブラウザ11を介して表示し、ユーザからの入力によって発注処理を行う発注処理部12を備える。一方、店舗装置2は、ユーザから送られてくる発注情報を解析して受注処理を行う受注処理部22を備える。

40 【0026】各認証局装置61、62、……6nは、契約をかわしたユーザ及び店舗に対してそれぞれ独立した公開鍵を発行する。したがって、あるユーザが2つの認証局61、6nと契約をした場合は、そのユーザは、2つの公開鍵を持つことになる。同様に店舗が複数の認証局と契約した場合には、その複数個分の公開鍵を持つことになる。ユーザと店舗とが共通の認証局CAと契約していて、その認証局CAが発行したユーザ及び店舗の公開鍵を利用することによって電子決裁が成立する。

50 【0027】図1の認証局リスト13、23は、ユーザ又は店舗がそれぞれ契約している認証局に関する情報を記憶したものである。2つの認証局61、62と契約したユーザ装置1に記憶される認証局リスト（客用）13には、認証局61および62を識別する情報と、この2つの認証局が発行したそのユーザを特定するための「公開鍵証明書」が少なくとも含まれる。たとえば、認証局リスト（客用）13には、ユーザ識別コード番号、ユーザの公開鍵、その公開鍵を発行した認証局の識別番号

クライアント
ユーザ装置
店舗装置

認証局のデジタル署名データが含まれる。認証局リスト（店舗用）23には、店舗識別コード番号、店舗の公開鍵、その公開鍵を発行した認証局の識別番号、認証局のデジタル署名データが含まれる。

【0028】発注処理部12及び受注処理部22は、通常CPU、ROM、RAM、タイマー、I/Oコントローラなどからなるマイクロコンピュータから構成され、認証局リスト13、23は、不揮発性のメモリ、たとえばハードディスクに記憶される。

【0029】以上のような基本構成を持つこの発明の認証システムは、ネットワークを介してユーザがある店舗に対して発注処理を実行した際に、ユーザ自らが同じ認証局と契約している店舗が否かを確認する操作をすることなしに、2つの「認証局リスト」13、23を利用して互いに共通な認証局を検索して、その共通の認証局を通した電子決裁を行なおうとするものである。

【0030】図2に、この発明の一実施例における発注処理部12及び受注処理部22の詳細な構成ブロック図を示す。ここで示した各手段は、ロジック回路や専用LSIを用いてハードウェア的に独立した構成としてもよいが、一般的に、拡張性等の点からマイクロコンピュータと各手段に対応したプログラムを組合わせて、各手段の機能を実行させるようにすることが好ましい。

【0031】また、認証局リスト13、23、注文伝票19及び見積もり伝票30、その他各手段が実行するのに必要なデータは、RAMやハードディスクなどに記憶される。WWWブラウザ11、WWWサーバ21は、インターネットにアクセスしてWWWの情報を表示、転送できるソフトウェアであればよく、市販されているソフトウェアを用いればよい。

【0032】ここで、認証局リスト13、23は、ユーザ又は店舗が契約した認証局から「公開鍵証明書」を受領したときに、ユーザ又は店舗の担当者がキーボード等を用いて必要なデータを入力することによって予め作成される。「公開鍵証明書」がフロッピーディスクなどの記憶媒体に入れられて発行される場合には、そのフロッピーディスクをユーザ又は店舗のパソコンに挿入し、所定の操作を行って自動的にデータを読み取って認証局リスト13、23を生成するようにしてもよい。

【0033】また、新たな認証局と契約した場合には、その都度その新たな認証局発行の「公開鍵証明書」に記載されたデータを入力することによって、認証局リスト13、23は更新される。すなわち、新たな認証局の情報が認証局リスト13、23に追加される。

【0034】店舗装置2の受注処理部22において、認証局リスト作成手段27は店舗が契約する認証局の一覧である認証局リスト（店舗用）23を作成し、データ受信手段26はWWWサーバ21から中継された注文伝票Cを復号化手段25に引き渡すものである。

【0035】復号化手段25は、注文伝票Cに添付され

たユーザの公開鍵を基に注文伝票を復号化し平文の注文内容を得、これを受注手段29に引き渡す。受注手段29は平文の注文内容に応じて受注処理を行う。ここで、受注処理には、ユーザの確認のため、認証局との間で行われる与信処理が含まれる。

【0036】伝票作成手段28は、WWWブラウザ21からの中継されたユーザからの注文内容に応じて、見積もり伝票Bを作成するものである。データ送信手段24は、認証局リスト（店舗用）23等をWWWサーバ21へ送るものである。WWWサーバ21は、WWWブラウザ11から送信された要求データに応答して、商品情報の送信、見積もり伝票Bの送信、認証局リスト（店舗用）23等の送信を行うものである。

【0037】ユーザ装置1は、WWWブラウザ11と発注処理部12からなる。WWWブラウザ11は、店舗装置2から送られてきた認証局リスト（店舗用）23と見積もり伝票Bを発注処理部12に中継するものである。発注処理部12において、認証局リスト作成手段18はユーザが契約する認証局の一覧である認証局リスト（客用）13を作成し、データ受信手段14はWWWブラウザ11から中継された認証局リスト（店舗用）23を認証局リスト比較手段15に、見積もり伝票Bを暗号化手段16に引き渡すものである。

【0038】認証局リスト比較手段15は、認証局リスト（客用）13と認証局リスト（店舗用）23を比較し、ユーザと店舗に共通な認証局aを決定する。暗号化手段16は、決定された認証局aの管理するこのユーザ固有の秘密鍵により注文内容を暗号化し、認証局aの発行する公開鍵を添付して注文伝票Cを作成し、注文伝票Cの送信データ送信手段17に依頼する。データ送信手段17は、注文伝票Cを店舗装置2に送信するものである。

【0039】図3に、この発明の一実施例における電子決裁の処理手順の説明図（シーケンス図）を示す。ステップS10からS13までの処理は、従来におけるステップS100からS103までの処理と同じであり、ユーザ1及び店舗2とも郵送等のオフライン手段によって認証局61から発行される「公開鍵証明書」を事前に取得する。ここで、ステップS22までの電子決裁が完了するためには、ユーザ1と店舗2とが少なくとも1つの共通の認証局と契約を結び、その認証局から発行された「公開鍵証明書」を取得する必要がある。

【0040】ステップS11、S13において「公開鍵証明書」が認証局から発行されるが、これには、通常この認証局の公開鍵が含まれる。含まれない場合は、たとえば別郵送にて発行してもよい。また、これとは別に、ユーザ1に対しては、認証局61が作成したユーザ1の秘密鍵が、店舗2に対しては、認証局61が作成した店舗2の秘密鍵が、その認証局から郵送等のオフライン手段によって発行される。ただし、この秘密鍵は、ユーザ

又は店舗が厳密に管理すべきものなので、認証局が発行する形態をとらずに、ユーザ又は店舗自身のプログラムで自動生成するようにしてもよい。

【0041】なお、「公開鍵証明書」のフォーマットは、I T U-TのX. 509で規定されたものを用いればよい。以上のステップS10からステップS13までのオフライン処理は、この認証システムを運用する上で前提となる処理であり、この手段を一回のみ行なえばよい。

【0042】ステップS14において、ユーザ1が、インターネット3を経由して、店舗2のWWWサーバ21にアクセスする。ステップS15において、店舗2が、このユーザ1に対してその店舗2の所有する商品情報等を送信する。ステップS16において、この商品情報を取得したユーザ1は、自己の望む商品あるいはサービスが決定したら、「発注意思表示」を示すデータを店舗2へ転送する。ここまでの処理は、図2におけるWWWブラウザ11、WWWサーバ21間の通信によって実行することが可能であり、転送されるデータは図2には図示していないが、ユーザ1及び店舗2の各装置中のハードディスク等にデータベースとして蓄積しておけばよい。

【0043】ステップS17において、店舗2では、この発注意思表示に対して、認証局リスト作成手段27によって作成されたこの店舗2が契約しているすべての認証局を含む認証局リスト（店舗用）23を、データ送信手段24を通してWWWサーバ21がユーザ1へ送信する。ユーザ1では、この認証局リスト（店舗用）23は、WWWブラウザ11で中継され、データ受信手段14によって受信される。

【0044】ステップS18において、さらに店舗2では、伝票作成手段26が見積もり伝票B30を作成し、データ送信手段24を通してWWWサーバ21がこの見積もり伝票B30を送信する。ユーザ1では、同様にしてこの見積もり伝票B30がデータ受信手段14によって受信されると、図示していない表示手段あるいは印刷手段等を利用してユーザ1に見積もり内容が提示される。

【0045】ステップS19において、ユーザ1で予め作成されていたユーザの認証局リスト（局用）13と、ステップS17で受信された認証局リスト（店舗用）23とを、認証局リスト比較手段15が比較し、電子決裁をするための認証局を選択する。

【0046】ここで、認証局リスト13及び23には、認証局の名称あるいは識別番号が含まれているので、両リストに同じものが含まれているかどうかを判断する。両リストに同じものが含まれていない場合には、電子決裁に必要な認証ができないことになり、残念ながら、この電子決裁は不成立となり、ユーザは商品等を購入できない。一方、両リストの一つでも同じ認証局が含まれている場合は、認証が可能であるため、この両リストに共通な認証局を選び出す。

【0047】共通の認証局が複数存在する場合には、その中から適当な一つを選べばよい。あるいは、複数の認証局を表示手段に表示して、ユーザに選択させるようにしてもよい。さらに後述するように、予め付与された選択優先度によって自動選択するようにしてもよい。

【0048】ステップS20において、認証を行う認証局が選択されれば、暗号化手段16が、ユーザを特定するカード番号及び選択された認証局の識別番号を含む注文伝票C19を暗号化して、データ送信手段17がWWWブラウザ11を介してこれらの暗号化された情報を店舗2へ送信する。このとき、暗号化には、ユーザ固有の秘密鍵や選択された認証局の公開鍵が使用される。

【0049】たとえば、ユーザを特定するカード番号は、認証局がユーザの身元が正しいかどうかを確認するものであるので、選択された認証局の公開鍵（ステップS11で発行されたもの）で暗号化すればよい。また、カード番号を除く注文伝票の情報、たとえば商品名、番号、数量、金額などは、店舗2が受注する際に必要となるものであるため、ユーザ固有の秘密鍵で暗号化すればよい。また、店舗2でこの暗号化された情報を解くために、ユーザの公開鍵も、通常、注文伝票の送信時に、ユーザ1から店舗2へ送信される。

【0050】ステップS21において、店舗2のデータ受信手段26が注文伝票Cを受信した後、復号化手段25が「カード番号」を除いた注文に関与する情報のみを抽出して復号化を行なう。この情報の復号化には、通常、送信されてきたユーザの公開鍵が用いられる。この復号化された情報は、受注手段29へ渡され、商品手配などの受注処理が実行される。

【0051】一方、店舗2において、ユーザの「カード番号」は、データ送信手段24によって認証局61へ送られる（ステップS22）。ここでの認証局61は、ユーザ1が選択した認証局であることは言うまでもない。また、「カード番号」は、まだ認証局61の公開鍵で暗号化されたままである。

【0052】ステップS23において、認証局61に送られてきたユーザの「カード番号」は、認証局61の秘密鍵を用いて復号化される。そして、認証局61は、ユーザの身元を認証した後、認証の可否（与信結果）を店舗2へ通知する。ステップS24において、この与信結果を受けた店舗2は、ユーザ1の認証が正常にできたと判断した場合には、利用明細書をユーザ1へ送信する。以上のようにして、この発明の一実施例の電子決裁が完了する。

【0053】ステップS20の暗号化には、現状では、RSAの公開鍵方式が最も広く使われているため、RSAの公開鍵方式を用いるのが好ましいが、RSA以外の公開鍵方式（例えば、BOSや楕円方式等）でも可能である。また、公開鍵方式だけでなく、公開鍵方式と共通鍵方式（例えば、FEALやMULT12、MIST

Y)と組み合わせた方式でも可能である。また、注文伝票を送信する方法としては、暗号化された伝票を電子メールで送る方法でもよい。

【0054】このように、ユーザも店舗も、複数の認証局と契約していた場合に、店舗側が契約しているすべての認証局のリストをユーザに通知するようにしているので、ユーザが、その店舗がどの認証局と契約しているかを確認する操作をすることなく、容易に電子決裁を行う認証局を選択することが可能となる。

【0055】この発明において、店舗側とユーザ側で同一の認証局と契約を結び、どちらも同じ認証局から発行される公開鍵証明書を手前に取得する電子決裁の形態を実施例として説明した。しかし、世界的にも電子決裁（電子商取引）はまだ実験段階であり、認証の方法はさまざまな形態が考えられる。また、実際の認証局の運営をクレジット会社が行う形態をとる場合には、当面は認証局が複数存在する可能性がある。このような場合に、特にこの発明の認証システムは有効に機能する。

【0056】図4、及び図5に、この発明の認証局リストの一実施例を示す。図4は、ユーザ装置1で作成される認証局リスト（客用）13の実施例である。図5は、店舗装置2で作成される認証局リスト（店舗用）23の実施例である。いずれも認証局を示す識別番号（a、b、……g）と、暗号化された各認証局が発行した「公開鍵証明書」の内容から構成される。

【0057】ここで、前記したステップS19では、認証局リスト比較手段15は、両リストの認証局の識別番号の中に一致するものがあるか否かを判断すればよい。また、図4に示すように、認証局リスト（客用）13には、選択優先度を付与してもよい。たとえば、認証局aの選択優先度を高く、認証局cの選択優先度を低くなるように数字を付与してもよい。図4では、ユーザが契約した認証局のうち、認証局aが最も選択優先度が高く、次に認証局dが高く、認証局cが最も選択優先度が低い。図4と図5を比較すると、両リストに共通する認証局は、“c”と“d”であることがわかる。

【0058】したがって、このリストの場合は認証局“c”又は“d”が選択されることになるが、複数の認証局が選択可能な場合は、最初に見つけた方を選択してもよい。また、選択優先度の最も高いものを優先して選ぶことにすると、図4のような優先度を付与した場合、認証を行う認証局としては、優先度の高い“d”の方が自動的に選択されることになる。なお、この選択の優先度付けは、ユーザが認証局リスト（客用）14を作成する際に、キーボード等の入力手段を利用して行なえばよい。

【0059】このように、予めユーザの契約した認証局に選択優先度を付与しておけば、電子決裁で利用可能な認証局が複数存在する場合でも、自動的に利用する認証局が一つ選択される。したがって、ユーザがその都度利

用する認証局を指定する必要がなくなるので、ユーザにとってスムーズな電子決裁手続をすることができる。

【0060】なお、上記の実施例では、ユーザ、店舗及び認証局がインターネットを介して接続された場合を示したが、この発明の認証システムは、他のWANやLANなどのネットワークでも実施できる。他のネットワークの場合には、通信プロトコルやデータフォーマットの形式をそのネットワークで規定されたものを使えばよく、図2に示した構成及び図3に示した処理手順はそのまま利用することができる。

【0061】

【発明の効果】この発明によれば、サービス提供サーバからクライアント装置へ、サービス提供サーバが契約している認証局のリストを送信するようにしているので、クライアント装置において、ユーザの契約している認証局とサービス提供サーバの契約している認証局とを比較して、利用する認証局を選択することができる。また、クライアント装置においてユーザが契約している認証局に選択優先度を付与するようにしているので、ユーザは、複数の認証局の中から利用する認証局をその都度選択する必要はなく、スムーズに電子決裁を行うことができる。

【図面の簡単な説明】

【図1】この発明の基本構成ブロック図である。

【図2】この発明の一実施例における構成ブロック図である。

【図3】この発明の一実施例における電子決裁の処理手順の説明図である。

【図4】この発明の認証局リスト（客用）の実施例を示す図である。

【図5】この発明の認証局リスト（店舗用）の実施例を示す図である。

【図6】従来の電子決裁の処理手順の説明図である。

【符号の説明】

- 1 ユーザ装置
- 2 店舗装置
- 11 WWWブラウザ
- 12 発注処理部
- 13 認証局リスト（客用）
- 14 データ受信手段
- 15 認証局リスト比較手段
- 16 暗号化手段
- 17 データ送信手段
- 18 認証局リスト作成手段
- 19 注文伝票C（カード番号）
- 21 WWWサーバ
- 22 受注処理部
- 23 認証局リスト（店舗用）
- 24 データ送信手段
- 25 復号化手段

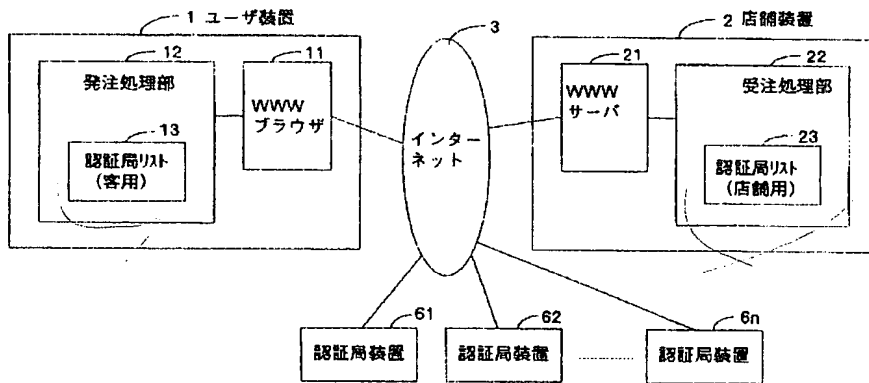
26 データ受信手段
27 認証局リスト作成手段
28 伝票作成手段

* 29 受注手段
30 見積もり伝票B
*

【図1】

【図5】

この発明の基本構成ブロック図



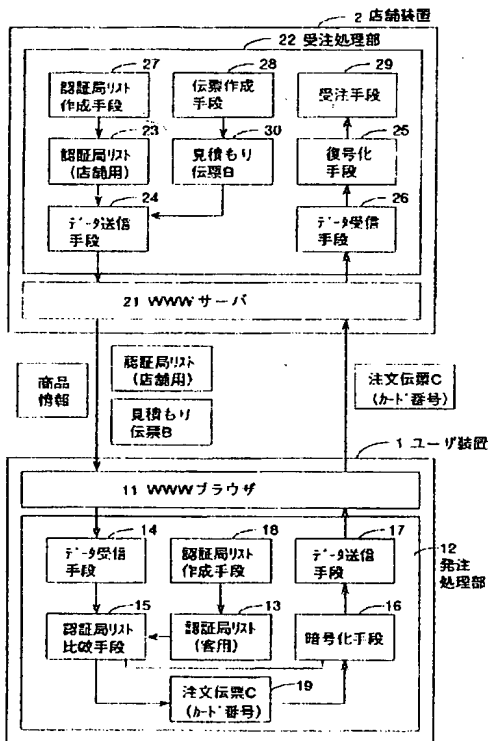
この発明の認証局リスト（店舗用）

認証局	証明書（暗号化）
b	公開鍵証明書（b局発行）
c	公開鍵証明書（c局発行）
d	公開鍵証明書（d局発行）
e	公開鍵証明書（e局発行）
f	公開鍵証明書（f局発行）
g	公開鍵証明書（g局発行）

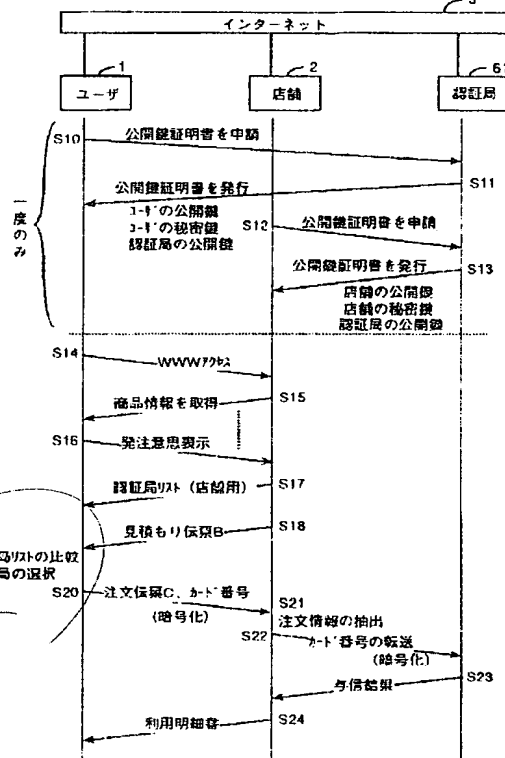
【図2】

【図3】

この発明の一実施例の構成ブロック図



この発明の電子決済の処理手順

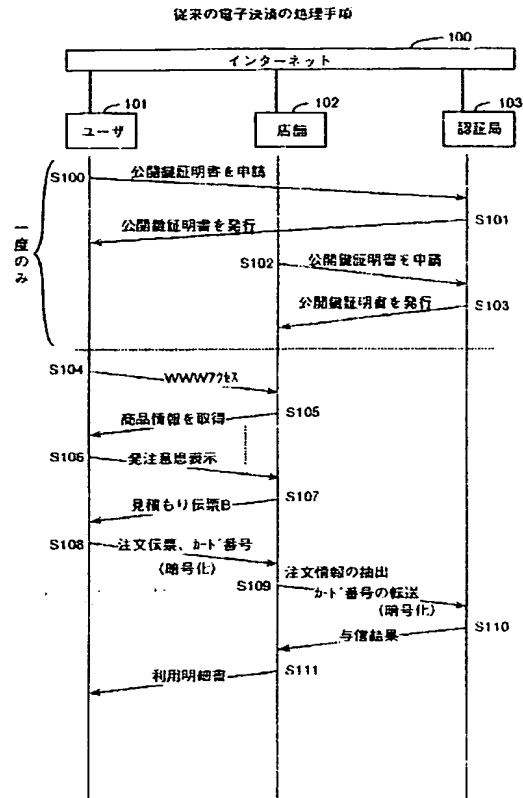


【図4】

この発明の認証局リスト（客用）

優先度	認証局	証明書（暗号化）
大 1	a	公開鍵証明書（a局発行）
2	d	公開鍵証明書（d局発行）
小 3	c	公開鍵証明書（c局発行）

【図6】



THIS PAGE BLANK (USPTO)